Sr.no.	Practical Def.	Page no.	Date	Sign
1.	To study about time division multiplexing.			
2.	To study of wireless ad hoc network and it’s working.			
3.	To study about different types of antenna in wireless communication.			
4.	To study about various multiple access scheme.			
5.	To study about Wi-Fi and the IEEE 802.11 Wireless LAN Standard.			
6.	To study about GSM architecture and signaling techniques.			
7.	To study about Cellular system and related concepts.			
8.	To study about GPRS services.			
9.	To study about Bluetooth architecture.			
10.	To study about Mobile IP.			

PRACTICAL 1

AIM: To study about time division multiplexing.

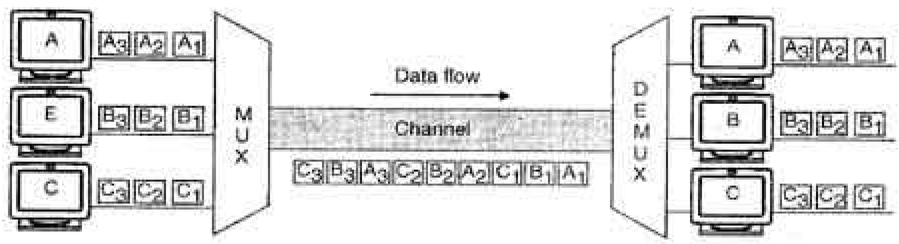
- In telecommunications and computer networks, **multiplexing** (sometimes contracted to **muxing**) is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share a scarce resource.

Types of Multiplexing

1. Space-division multiplexing
2. Frequency-division multiplexing
3. **Time-division multiplexing**
4. Code-division multiplexing

Time Division Multiplexing

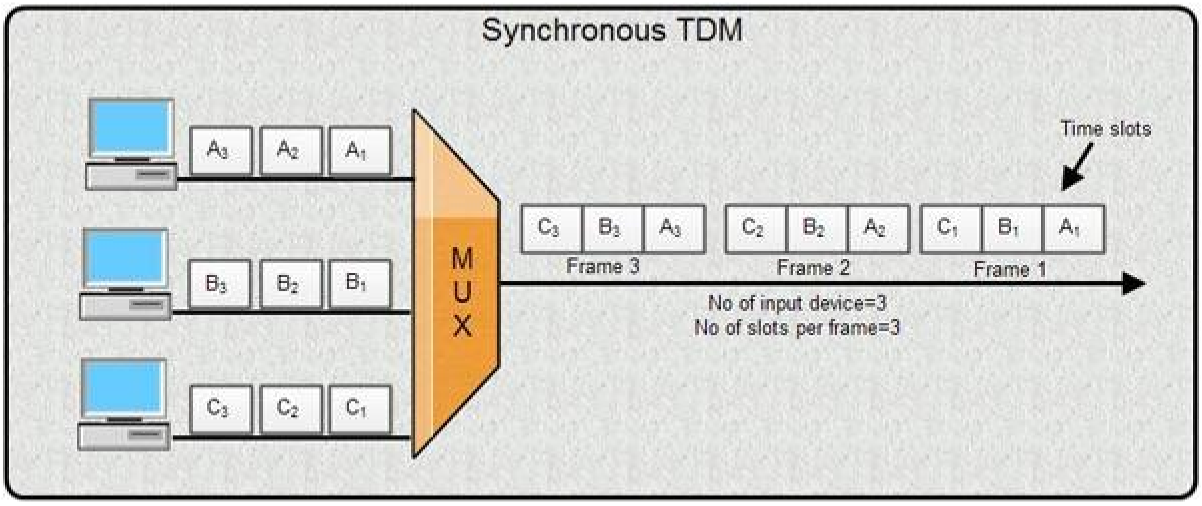
1. TDM is the digital multiplexing technique.
2. In TDM, the channel/link is not divided on the basis of frequency but on the basis of time.
3. Total time available in the channel is divided between several users.
4. Each user is allotted a particular a time interval called time slot or time slice during which the data is transmitted by that user.
5. Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time.
6. In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices.
7. In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one.
8. Thus each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel.
9. The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing.
10. The TDM signal in the form of frames is transmitted on the common communication medium.



Time Division Multiplexing (TDM)

Types of TDM
1. Synchronous TDM
2. Asynchronous TDM

Synchronous TDM (STDM)
1. In synchronous TDM, each device is given same **time slot** to transmit the data over the link, irrespective of the fact that the device has any data to transmit or not. Hence the name Synchronous TDM. Synchronous TDM requires that the total speed of various input lines should not exceed the capacity of path.
2. Each device places its data onto the link when its **time slot** arrives *i.e.* each device is given the possession of line turn by turn.



3. If any device does not have data to send then its time slot remains empty.
4. The various time slots are organized into **frames** and each frame consists of one or more time slots dedicated to each sending device.
5. If there are *n* sending devices, there will be *n* slots in frame *i.e.* one slot for each device.
6. As show in fig, there are 3 input devices, so there are 3 slots in each frame.

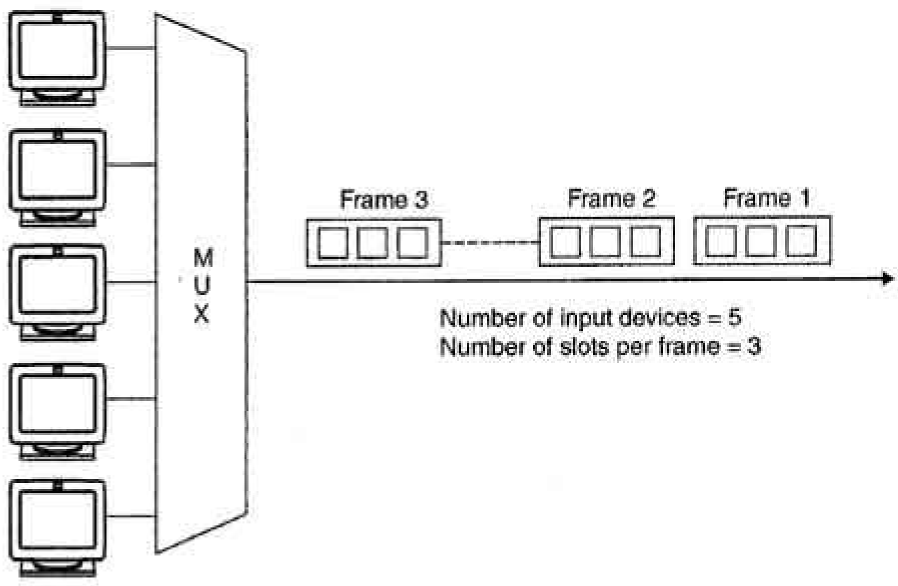
Disadvantages of Synchronous TDM

1. The channel capacity cannot be fully utilized. Some of the slots go empty in certain frames. As shown in fig only first two frames are completely filled. The last three frames have 6 empty slot. It means out of 20 slots in all, 6 slots are empty. This wastes the l/4th capacity of links.

2. The capacity of single communication line that is used to carry the various transmission should be greater than the total speed of input lines.

Asynchronous TDM

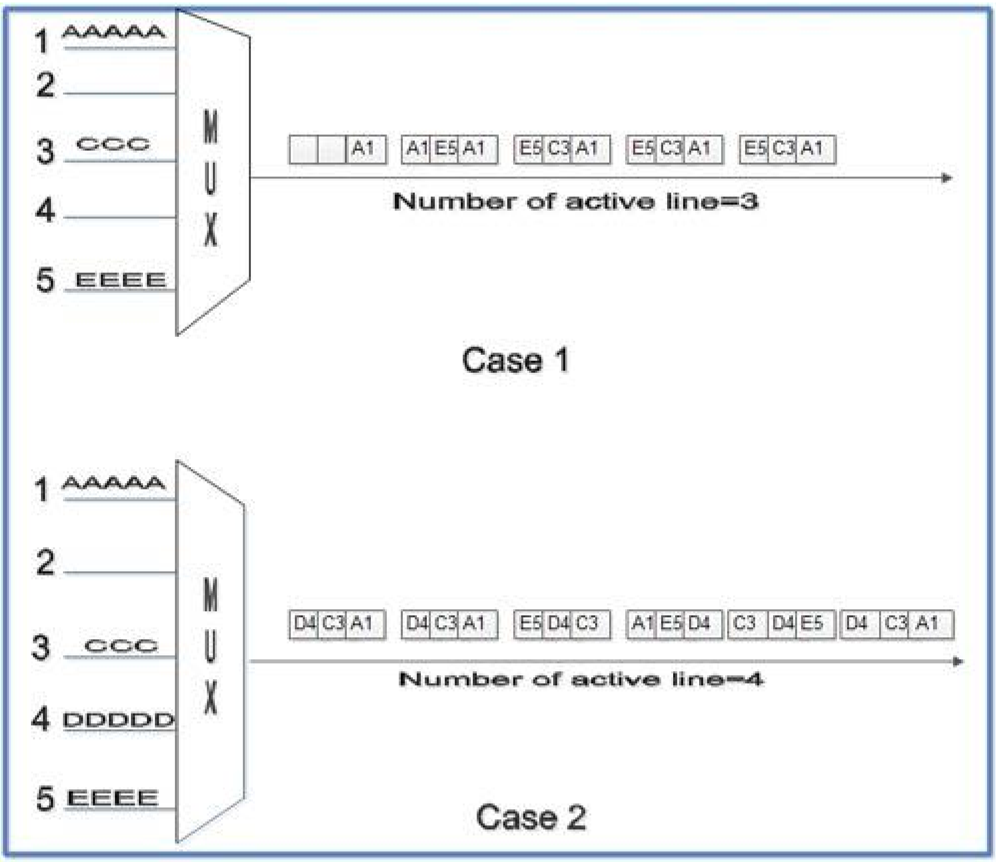
1. It is also known as statistical time division multiplexing.
2. Asynchronous TDM is called so because is this type of multiplexing, time slots are not fixed *i.e.* the slots are flexible.
3. Here, the total speed of input lines can be greater than the capacity of the path.
4. In synchronous TDM, if we have n input lines then there are n slots in one frame. But in asynchronous it is not so.
5. In asynchronous TDM, if we have n input lines then the frame contains not more than m slots, with m less than n $(m < n)$.
6. In asynchronous TDM, the number of time slots in a frame is based on a statistical analysis of number of input lines.
7. In this system slots are not predefined, the slots are allocated to any of the device that has data to send.
8. The multiplexer scans the various input lines, accepts the data from the lines that have data to send, fills the frame and then sends the frame across the link.

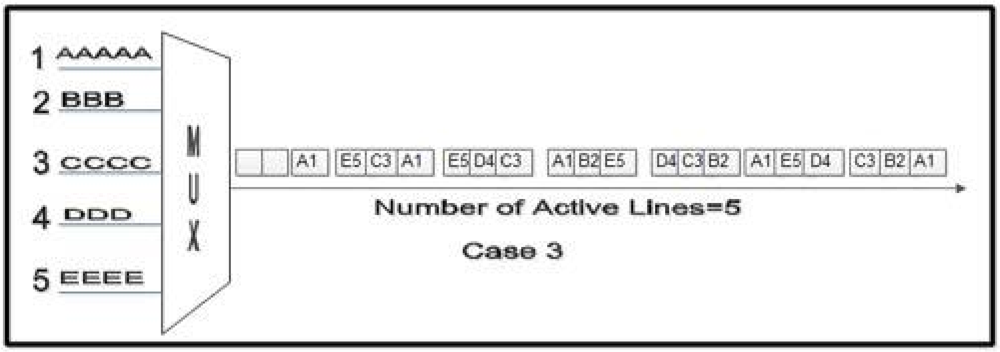


Asynchronous TDM

9. If there are not enough data to fill all the slots in a frame, then the frames are transmitted partially filled.
10. Asynchronous Time Division Multiplexing is depicted in fig. Here we have five input lines and three slots per frame.
11. In Case 1, only three out of five input lines place data onto the link *i.e.* number of input lines and number of slots per frame are same.
12. In Case 2, four out of five input lines are active. Here number of input line is one more than the number of slots per frame.
13. In Case 3, all five input lines are active.
In all these cases, multiplexer scans the various lines in order and fills the frames and transmits them across the channel.

The distribution of various slots in the frames is not symmetrical. In case 2, device 1 occupies first slot in first frame, second slot in second frame and third slot in third frame.





Advantages of TDM

1. Full available channel bandwidth can be utilized for each channel.
2. Intermodulation distortion is absent.
3. TDM circuitry is not very complex.
4. The problem of crosstalk is not severe.

Disadvantages of TDM

1. Synchronization is essential for proper operation.
2. Due to slow narrowband fading, all the TDM channels may get wiped out.

PRACTICAL 2

AIM: To study of wireless ad hoc network and it's working.

- The current cellular wireless networks are classified as the
  1. Infrastructure - dependent network.
  2. Infrastructure - less network (Ad – hoc network).

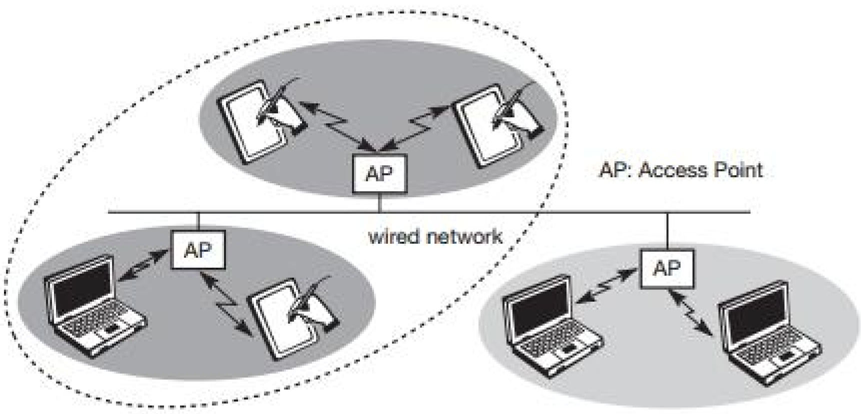
1. Infrastructure – Dependent Network

Many WLANs of today need an infrastructure network. Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control etc. In these infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes.

The access point does not just control medium access, but also acts as a bridge to other wireless or wired networks. Figure shows three access points with their three wireless networks and a wired network. Several wireless networks may form one logical wireless network, so the access points together with the fixed network in between can connect several wireless networks to form a larger network beyond actual radio coverage.

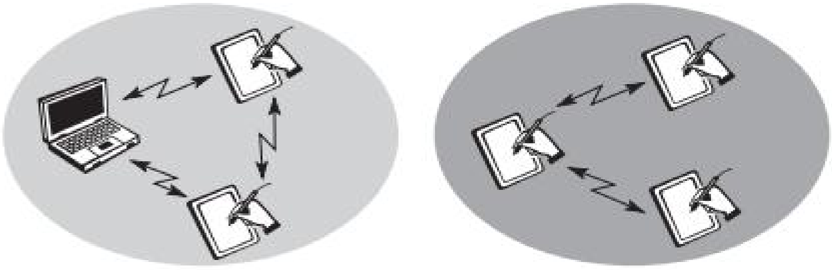
Typically, the design of infrastructure-based wireless networks is simpler because most of the network functionality lies within the access point, whereas the wireless clients can remain quite simple. This structure is reminiscent of switched Ethernet or other star-based networks, where a central element (e.g., a switch) controls network flow.

This type of network can use different access schemes with or without collision. Collisions may occur if medium access of the wireless nodes and the access point is not coordinated. However, if only the access point controls medium access, no collisions are possible. This setting may be useful for quality of service guarantees such as minimum bandwidth for certain nodes. The access point may poll the single wireless nodes to ensure the data rate.



2. Infrastructure - less network (Ad – hoc network).

Ad-hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary. Figure 2 shows two ad-hoc networks with three nodes each. Nodes within an ad-hoc network can only communicate if they can reach each other physically, i.e., if they are within each other's radio range or if other nodes can forward the message. Nodes from the two networks shown in Figure 2 cannot, therefore, communicate with each other if they are not within the same radio range. In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms, mechanisms to handle hidden or exposed terminal problems, and perhaps priority mechanisms, to provide a certain quality of service. This type of wireless network exhibits the greatest possible flexibility as it is, for example, needed for unexpected meetings, quick replacements of infrastructure or communication scenarios far away from any infrastructure.



Infrastructure less network (Ad – hoc network)

ISSUES IN AD HOC WIRELESS NETWORKS

The major issues that affect the design, deployment, & performance of an ad hoc wireless network system are:

1. Medium Access Scheme.
2. Transport Layer Protocol.
3. Routing.
4. Multicasting.
5. Energy Management.
6. Self-Organization.
7. Security.
8. Addressing & Service discovery.
9. Deployment considerations.
10. Scalability.
11. Pricing Scheme.
12. Quality of Service Provisioning

APPLICATIONS OF AD HOC WIRELESS NETWORKS

Military Application

Ad - hoc networks can be used to establish communication among a group of soldiers for tactical operations. Setting up of a fixed infrastructure for communication among group of soldiers in enemy territories (or in inhospitable terrains) may not be possible. In such a case, ad- hoc networks can be used to provide required communication quickly.

The military application enforces following requirements

  - Reliability
  - Efficiency
  - Secure communication
  - Support for multicast routing

Collaborative & Distributed Computing

- Ad -hoc network can be used to establish temporary communication infrastructure among a group of people in a conference.
- In distributed file sharing application, reliability is of high importance which would be provided by ad - hoc network.
- Other applications such as streaming of multimedia objects require support for soft real-time communication.
- Devices used can be
  - Laptops with add-on wireless interface cards
  - Enhanced PDA (Personal Digital Assistant) or
  - Mobile devices with high processing power

Wireless Sensor Networks (WSN)

- These are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.
- Sensor-nodes are tiny devices that have capability of
  - Sensing physical parameters
  - Processing the data gathered &
  - Communicating to the monitoring system

Bluetooth

Bluetooth can provide short range communication between the nodes such as a laptop and mobile phone.

Emergency Operations

Ad hoc wireless networks are functional in disaster operations such as searching operation and rescue operation and mob control.

PRACTICAL 3

AIM: To study about different types of antenna in wireless communication.

- An antenna can be defined as an electrical conductor or system of conductors used either for radiating electromagnetic energy or for collecting electromagnetic energy. In two-way communication, the same antenna can be and often is used for both transmission and reception.

An antenna will radiate power in all directions but, typically, does not perform equally well in all directions. A common way to characterize the performance of an antenna is the radiation pattern.

Radiation Pattern

Radiation pattern is a graphical representation of the radiation properties of an antenna as a function of space coordinates. The simplest pattern is produced by an idealized antenna known as the isotropic antenna. An **isotropic antenna** is a point in space that radiates power in all directions equally. The actual radiation pattern for the isotropic antenna is a sphere with the antenna at the center. However, radiation patterns are almost always depicted as a two-dimensional cross section of the three-dimensional pattern. The pattern for the isotropic antenna is shown in Figure l-a. The distance from the antenna to each point on the radiation pattern is proportional to the power radiated from the antenna in that direction. Figure l-b shows the radiation pattern of another idealized antenna. This is a directional antenna in which the preferred direction of radiation is along one axis.

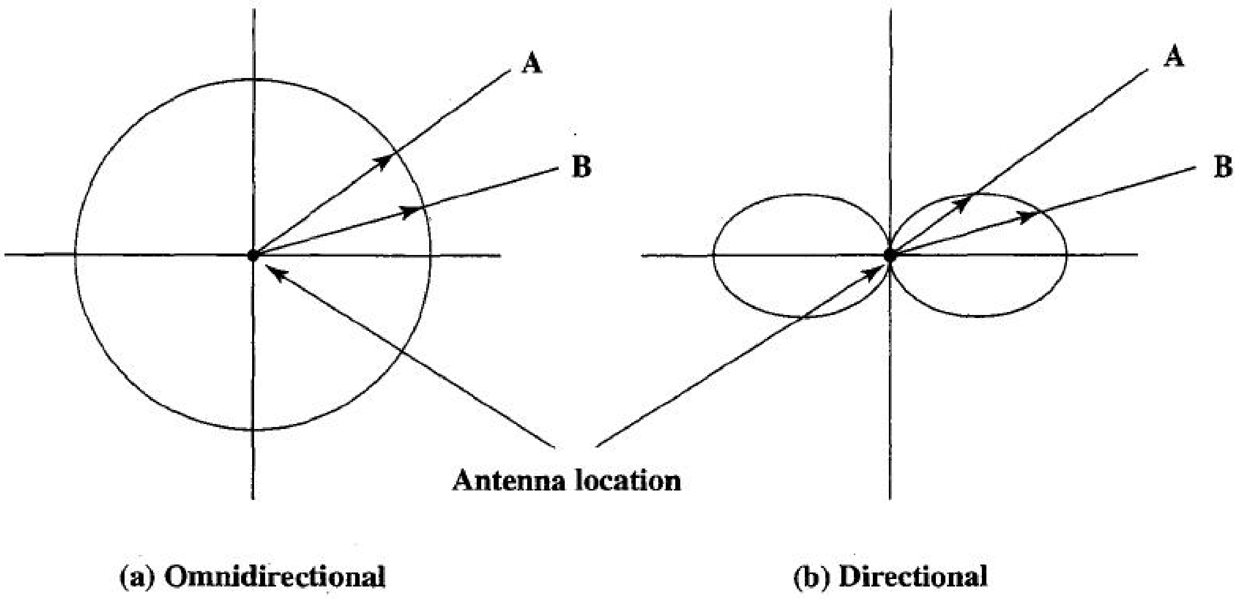


Figure 1: Idealized radiation pattern

The actual size of a radiation pattern is arbitrary. What is important is the relative distance from the antenna position in each direction. Figure 1 shows a comparison of two transmission angles, A and B, drawn on the two radiation patterns. The isotropic

antenna produces an omnidirectional radiation pattern of equal strength in all directions, so the A and B vectors are of equal length. For the antenna pattern of Figure l-b, the B vector is longer than the A vector, indicating that more power is radiated in the B direction than in the A direction, and the relative lengths of the two vectors are proportional to the amount of power radiated in the two directions.
When an antenna is used for reception, the radiation pattern becomes a **reception pattern.** The longest section of the pattern indicates the best direction for reception.

Antenna Types

1) Dipoles antenna
2) Parabolic antenna
3) Printed antenna
4) Adaptive antenna

1) Dipoles Antenna

Dipoles two of the simplest and most basic antennas are the half-wave dipole, or Hertz, antenna (Figure 2-a) and the quarter-wave vertical, or Marconi, antenna (Figure 2-b). The half-wave dipole consists of two straight collinear conductors of equal length, separated by a small gap. The length of the antenna is one-half the wavelength of the signal that can be transmitted most efficiently. A vertical quarter wave antenna is the type commonly used for automobile radios and portable radios.

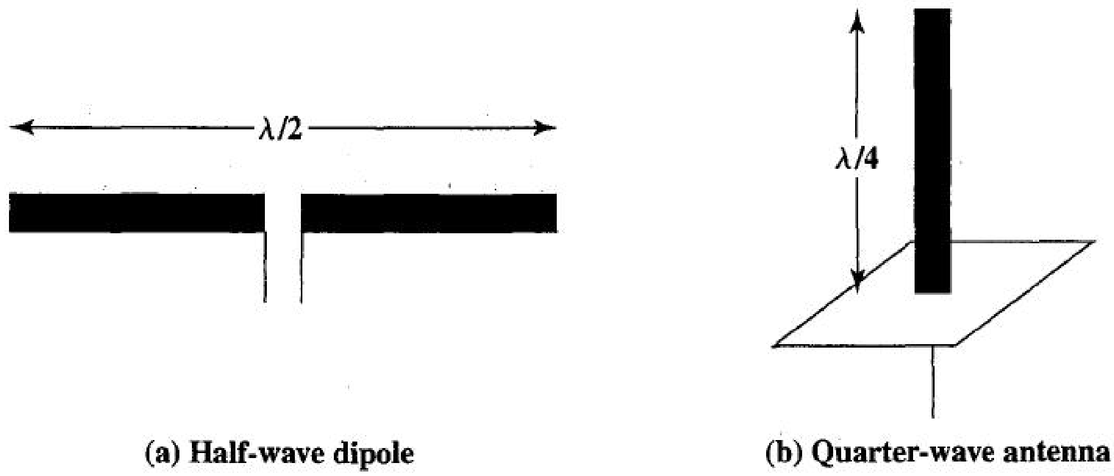


Figure 2: Simple antennas

A half-wave dipole has a uniform or omnidirectional radiation pattern in one dimension and a figure eight pattern in the other two dimensions (Figure 3-a). More complex antenna configurations can be used to produce a directional beam.

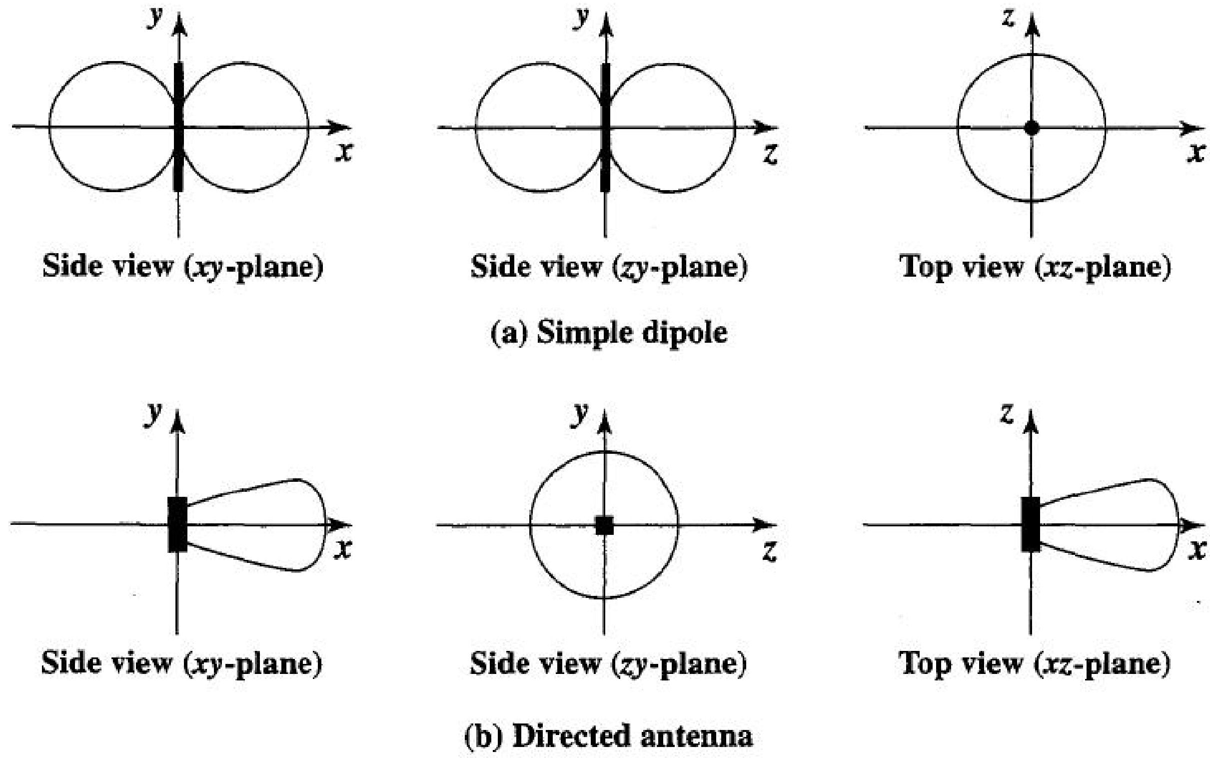


Figure 3: Radiation pattern in three dimension

A typical directional radiation pattern is shown in Figure 5.3b. In this case the main strength of the antenna is in the x-direction.

2) Parabolic antenna

An important type of antenna is the **parabolic reflective antenna,** which is used in terrestrial microwave and satellite applications. A parabola is the locus of all points equidistant from a fixed line and a fixed point not on the line. The fixed point is called the *focus* and the fixed line is called the *directrix* (Figure 4-a). If a parabola is revolved about its axis, the surface generated is called a *paraboloid.* A cross section through the paraboloid parallel to its axis forms a parabola and a cross section perpendicular to the axis forms a circle. Such surfaces are used in automobile headlights, optical and radio telescopes, and microwave antennas because of the following property: If a source of electromagnetic energy (or sound) is placed at the focus of the paraboloid, and if the paraboloid is a reflecting surface, then the wave will bounce back in lines parallel to the axis of the paraboloid; Figure 4-b shows this effect in cross section. In theory, this effect creates a parallel beam without dispersion. In practice, there will be some dispersion, because the source of energy must occupy more than one point. The converse is also true. If incoming waves are parallel to the axis of the reflecting paraboloid, the resulting signal will be concentrated at the focus.

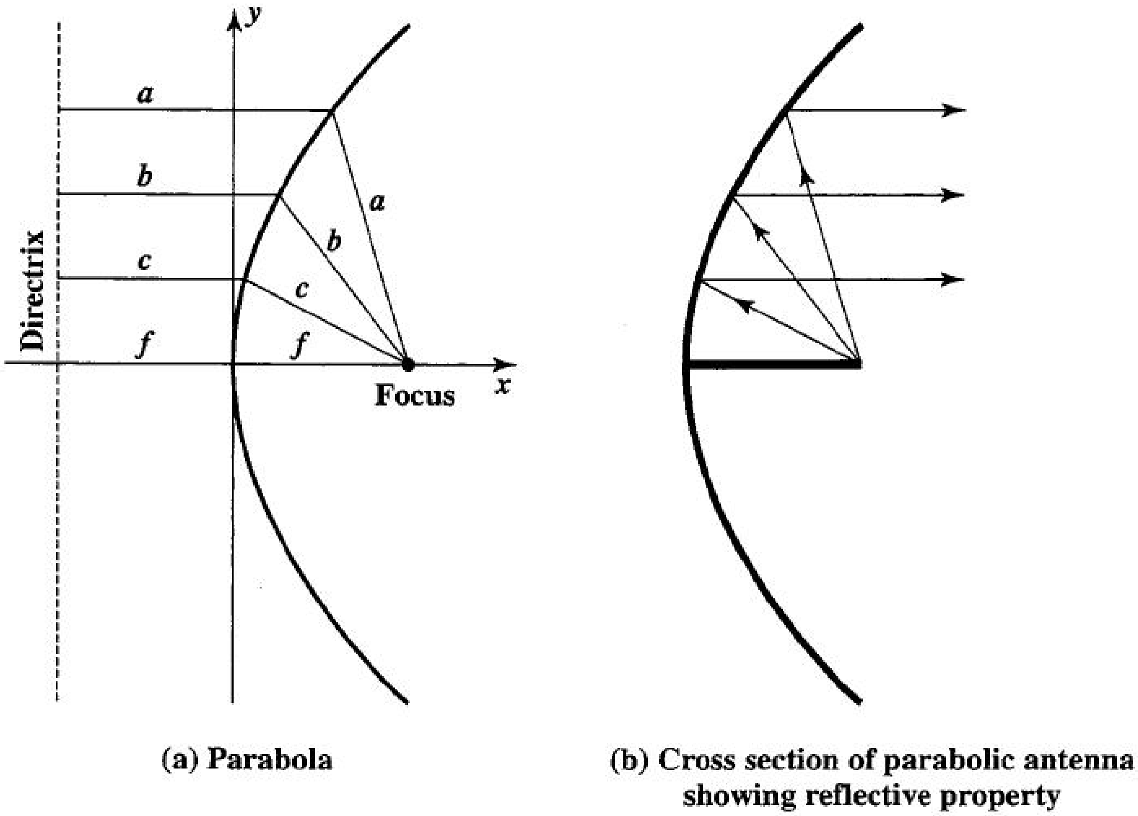


Figure 4: Parabolic antenna

3) Printed antenna

This type of antenna is popular for applications requiring:

- Planar antennas.
- Efficient radiators.
- Arrays for low or medium directivity.
- 2 GHz upwards.
- Lightweight, simple construction and cost effectiveness.

The communications group has facilities for complete prototyping of printed antennas of almost any geometry. Popular designs include ISM band arrays (medium gain antennas at 2.45 GHz and also 5.85 GHz). A 12 element 2.45 GHz uniform array is shown below, which offers 12 dBi of gain.

Overall dimensions are 300 x 200 mm. The substrate used is a low-loss microwave laminate of thickness 0.79 mm and dielectric constant 3.2 The radiation patterns are fully characterized.

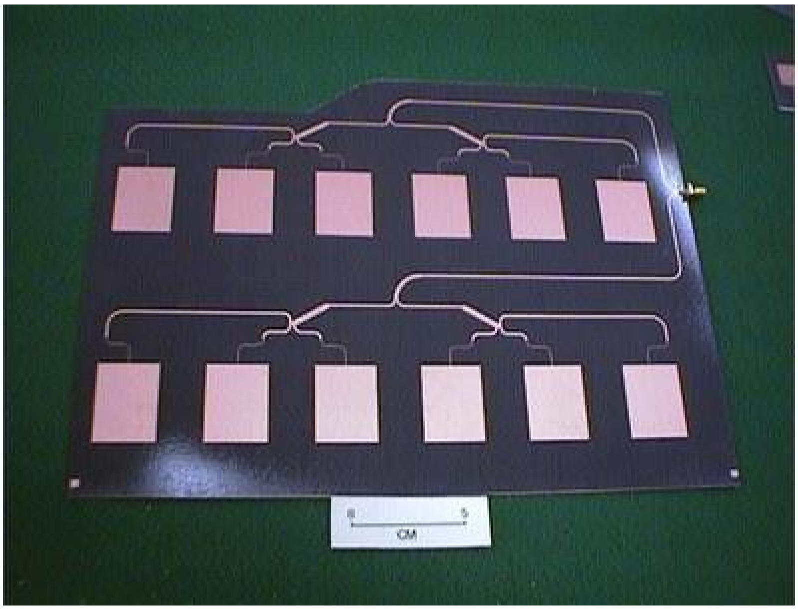


Figure 5: Printed antenna

4) Adaptive antenna

Smart antennas (also known as adaptive array antennas, digital antenna arrays, multiple antennas and, recently, MIMO) are antenna arrays with smart signal processing algorithms used to identify spatial signal signatures such as the direction of arrival (DOA) of the signal, and use them to calculate beamforming vectors which are used to track and locate the antenna beam on the mobile/target. Smart antennas should not be confused with reconfigurable antennas, which have similar capabilities but are single element antennas and not antenna arrays.

Smart antenna techniques are used notably in acoustic signal processing, track and scan radar, radio astronomy and radio telescopes, and mostly in cellular systems like W-CDMA, UMTS, and LTE.

Smart antennas have many functions: DOA estimation, beamforming, interference nulling, and constant modulus preservation.

Figure 6: Smart / Adaptive antenna

PRACTICAL 4

AIM : To study about various multiple access scheme.

- Multiple access schemes are used to allow many mobile users to share simultaneously a finite amount of radio spectrum.

Multiple Access Techniques

In wireless communication systems, it is often desirable to allow the subscriber to send information simultaneously from the mobile station to the base station while receiving information from the base station to the mobile station.

A cellular system divides any given area into cells where a mobile unit in each cell communicates with a base station. The main aim in the cellular system design is to be able to **increase the capacity of the channel**, i.e., to handle as many calls as possible in a given bandwidth with a sufficient level of quality of service.

There are several different ways to allow access to the channel. These includes mainly the following −

- Frequency division multiple-access (FDMA)
- Time division multiple-access (TDMA)
- Code division multiple-access (CDMA)
- Space division multiple access (SDMA)

Depending on how the available bandwidth is allocated to the users, these techniques can be classified as **narrowband** and **wideband** systems.

Narrowband Systems

Systems operating with channels substantially narrower than the coherence bandwidth are called as Narrow band systems. Narrow band TDMA allows users to use the same channel but allocates a unique time slot to each user on the channel, thus separating a small number of users in time on a single channel.

Wideband Systems

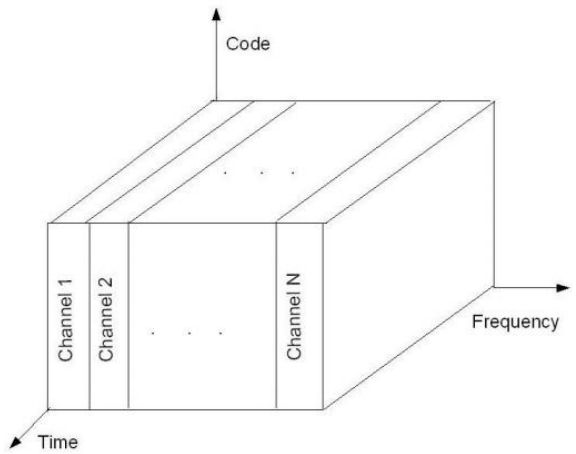
In wideband systems, the transmission bandwidth of a single channel is much larger than the coherence bandwidth of the channel. Thus, multipath fading doesn't greatly affect the received signal within a wideband channel, and frequency selective fades occur only in a small fraction of the signal bandwidth.

Frequency Division Multiple Access (FDMA)

FDMA is the basic technology for advanced mobile phone services. The features of FDMA are as follows.

- FDMA allots a different sub-band of frequency to each different user to access the network.
- If FDMA is not in use, the channel is left idle instead of allotting to the other users.

- FDMA is implemented in Narrowband systems and it is less complex than TDMA.
- Tight filtering is done here to reduce adjacent channel interference.
- The base station BS and mobile station MS, transmit and receive simultaneously and continuously in FDMA.



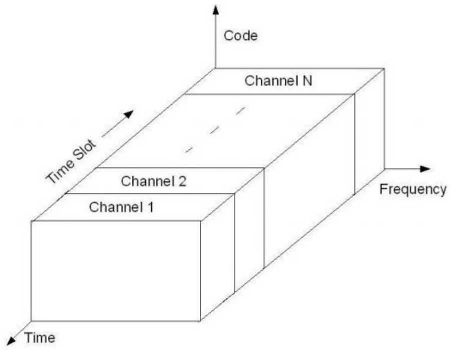
FDMA/FDD in AMPS

The first U.S. analog cellular system, AMPS (Advanced Mobile Phone System) is based on FDMA/FDD. A single user occupies a single channel while the call is in progress, and the single channel is actually two simplex channels which are frequency duplexed with a 45 MHz split. When a call is completed or when a handoff occurs the channel is vacated so that another mobile subscriber may use it.

Time Division Multiple Access (TDMA)

In the cases where continuous transmission is not required, there TDMA is used instead of FDMA. The features of TDMA include the following.

- TDMA shares a single carrier frequency with several users where each users makes use of non-overlapping time slots.
- Data transmission in TDMA is not continuous, but occurs in bursts. Hence handoff process is simpler.
- TDMA uses different time slots for transmission and reception thus duplexers are not required.
- TDMA has an advantage that is possible to allocate different numbers of time slots per frame to different users.
- Bandwidth can be supplied on demand to different users by concatenating or reassigning time slot based on priority.



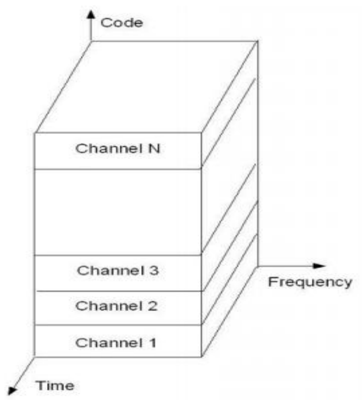
TDMA/FDD in GSM

As discussed earlier, GSM is widely used in Europe and other parts of the world. GSM uses a variation of TDMA along with FDD. GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band. Since many GSM network operators have roaming agreements with foreign operators, users can often continue to use their mobile phones when they travel to other countries.

Code Division Multiple Access (CDMA)

Code division multiple access technique is an example of multiple access where several transmitters use a single channel to send information simultaneously. Its features are as follows.

- In CDMA every user uses the full available spectrum instead of getting allotted by separate frequency.
- CDMA is much recommended for voice and data communications.
- While multiple codes occupy the same channel in CDMA, the users having same code can communicate with each other.
- CDMA offers more air-space capacity than TDMA.
- The hands-off between base stations is very well handled by CDMA.



CDMA/FDD in IS-95

In this standard, the frequency range is: 869-894 MHz (for Rx) and 824-849 MHz (for Tx). In such a system, there are a total of 20 channels and 798 users per channel. For each channel, the bit rate is 1.2288 Mbps. For orthogonally, it usually combines 64 Walsh-Hadamard codes and an m-sequence.

Space Division Multiple Access (SDMA)

Space division multiple access or spatial division multiple access is a technique which is MIMO (multiple-input multiple-output) architecture and used mostly in wireless and satellite communication. It has the following features.

- All users can communicate at the same time using the same channel.
- SDMA is completely free from interference.
- A single satellite can communicate with more satellites receivers of the same frequency.
- The directional spot-beam antennas are used and hence the base station in SDMA, can track a moving user.
- Controls the radiated energy for each user in space.

PRACTICAL 5

AIM: To study about Wi-Fi and the IEEE 802.11 Wireless LAN Standard.

- Figure 5.1 illustrates the model developed by the 802.11 working group. The smallest building block of a wireless LAN is a basic service set (BSS), which consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium. A BSS may be isolated or it may connect to a backbone distribution system (DS) through an access point (AP). The AP functions as a bridge and a relay point. In a BSS, client stations do not communicate directly with one another. Rather, if one station in the BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from the originating station to the AP, and then from the AP to the destination station. Similarly, a MAC frame from a station in the BSS to a remote station is sent from the local station to the AP and then relayed by the AP over the DS on its way to the destination station. The BSS generally corresponds to what is referred to as a cell in the literature. The DS can be a switch, a wired network, or a wireless network.

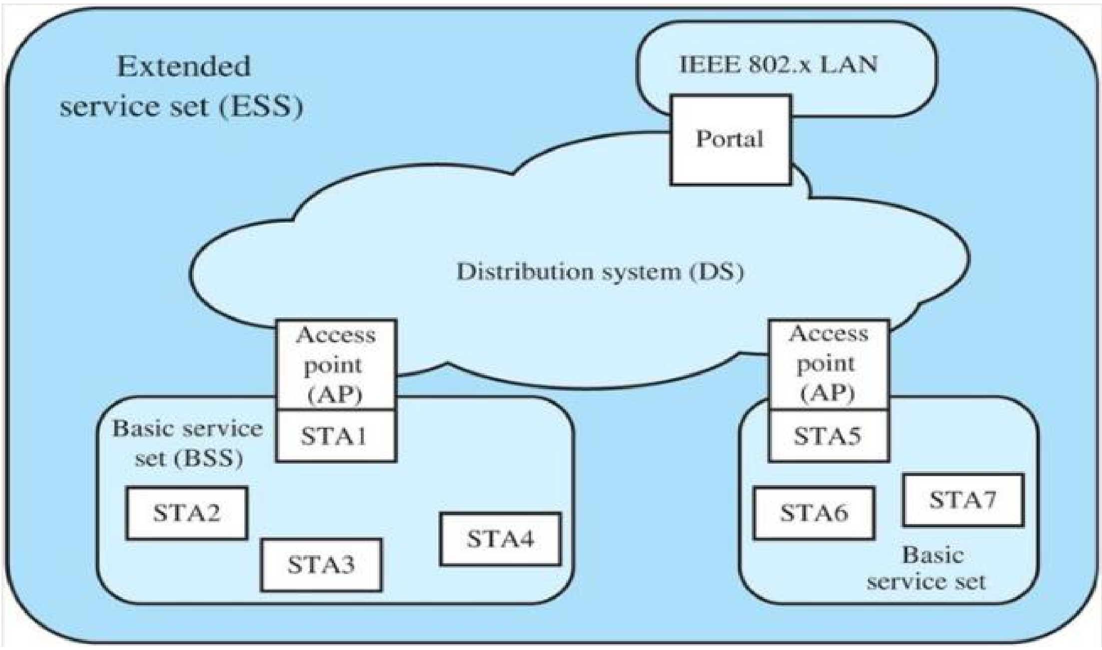


Figure 5.1: 802.11 architecture

When all the stations in the BSS are mobile stations, with no connection to other BSSs, the BSS is called an independent BSS (IBSS). An IBSS is typically an ad hoc network. In an IBSS, the stations all communicate directly, and no AP is involved.

A simple configuration is shown in Figure 14.4, in which each station belongs to a single BSS; that is, each station is within wireless range only of other stations within the same BSS. It is also possible for two BSSs to overlap geographically, so that a single station could participate in more than one BSS. Further, the association between a station and a BSS is dynamic. Stations may turn off, come within range, and go out of range.

An **extended service set (ESS)** consists of two or more basic service sets interconnected by a distribution system. Typically, the distribution system is a wired backbone LAN but can be any communications network. The extended service set appears as a single logical LAN to the logical link control (LLC) level.
Figure 5.1 indicates that an access point (AP) is implemented as part of a station; the AP is the logic within a station that provides access to the DS by providing DS services in addition to acting as a station. To integrate the IEEE 802.11 architecture with a traditional wired LAN, a **portal** is used. The portal logic is implemented in a device, such as a bridge or router, that is part of the wired LAN and that is attached to the DS.

802.11 Standards

IEEE 802.11 a
Channel Structure IEEE 802.11a makes use of the frequency band called the Universal Networking Information Infrastructure (UNNI), which is divided into three parts. The UNNI-1 band (5.15 to 5.25 GHz) is intended for indoor use; the UNNI-2 band (5.25 to 5.35 GHz) can be used either indoor or outdoor, and the UNNI-3 band (5.725 to 5.825 GHz) is for outdoor use.
IEEE 80211.a has several advantages over IEEE 802.11b/g:

- IEEE 802.lIa utilizes more available bandwidth than 802.11b/g. Each UNNI band provides four non overlapping channels for a total of 12 across the allocated spectrum.
- IEEE 802.lIa provides much higher data rates than 802.lIb and the same maximum data rate as 802.lIg.
- IEEE 802.lIa uses a different, relatively uncluttered frequency spectrum (5 GHz).

IEEE 802.11 b
IEEE 802.11b is an extension of the IEEE 802.11 DSSS scheme, providing data rates of 5.5 and 11 Mbps in the ISM band. The chipping rate is 11 MHz, which is the same as the original DSSS scheme, thus providing the same occupied bandwidth. To achieve a higher data rate in the same bandwidth at the same chipping rate, a modulation scheme known as complementary code keying (CCK) is used.
IEEE 802.11 c
IEEE 802.11 c is concerned with bridge operation. A bridge is a device that links two LANs that have a similar or identical MAC protocol. It performs functions similar to those of an IP-Level router, but at the MAC layer. Typically, a bridge is simpler and more efficient than an IP router. The 802.11c task group completed its work on this standard in 2003, and it was folded into the IEEE 802.11 d standard for LAN bridges.
IEEE 802.1 d

IEEE 802.11d is referred to as a regulatory domain update. It deals with issues related to regulatory differences in various countries.

IEEE 802.11 e

IEEE 802.11 e makes revisions to the MAC layer to improve quality of service and address some security issues. It accommodates time-scheduled and polled communication during null periods when no other data is being sent. In addition, it offers improvements to the efficiency of polling and enhancements to channel robustness. These enhancements should provide the quality required for such services as IP telephony and video streaming. Any station implementing 802.11e is referred to as a QoS station, or QSTA. In a QSTA, the DCF and PCF modules are replaced with a hybrid coordination function (HCF), which in tum consists of enhanced distributed channel access (EDCA) and HCF controlled channel access (HCCA). EDCA is an extension of the legacy DCF mechanism to include priorities. As with the PCF, HCCA centrally manages medium access, but does so in a more efficient and flexible manner.

IEEE 802.1l f

IEEE 802.11 f addresses the issue of interoperability among access points (APs) from multiple vendors. In addition to providing communication among WLAN stations in its area, an AP can function as a bridge that connects two 802.11 LANs across another type of network, such as a wired LAN (e.g., Ethernet) or a wide area network. This standard facilitates the roaming of a device from one AP to another while insuring continuity of transmission.

IEEE 802.11 h

IEEE 802.11 h deals with spectrum and power management issues. The objective is to make 802.11a products compliant with European regulatory requirements. In the EU, part of the 5-GHz band is used by the military for satellite communications. The standard includes a dynamic channel selection mechanism to ensure that the restricted portion of the frequency band is not selected. The standard also includes transmit power control features to adjust power to EU requirements.

IEEE 802.11 i

IEEE 802.11 I defines security and authentication mechanisms at the MAC layer. This standard is designed to address security deficiencies in the wire equivalent privacy (WEP) mechanism originally designed for the MAC layer of 802.1I. The 802.11i scheme uses stronger encryption and other enhancements to improve security.

IEEE 802.11 k

IEEE 802.11 k defines Radio Resource Measurement enhancements to provide mechanisms to higher layers for radio and network measurements. The standard defines what information should be made available to facilitate the management and maintenance of a wireless and mobile LANs. Among the data provided are the following:

- To improve roaming decisions, an AP can provide a site report to a station when it determines that the station is moving away from it. The site report is an ordered list of APs, from best to worst service that a station can use in changing over to another AP.

- An AP can collect channel information from each station on the WLAN. Each station provides a noise histogram that displays all non-802.11 energy on that channel as perceived by the station. The AP also collects statistics on how long a channel is used during a given time. These data enable the AP to regulate access to a given channel.
- APs can query stations to collect statistics, such as retries, packets transmitted, and packets received. This gives the AP a more complete view of network performance.
- 802.11k extends the transmit power control procedures defined in 802.11h to other regulatory domains and frequency bands, to reduce interference and power consumption and to provide range control.

IEEE 802.11 m

IEEE 802.11 m is an ongoing task group activity to correct editorial and technical issues in the standard. The task group reviews documents generated by the other task groups to locate and correct inconsistencies and errors in the 802.11 standard and its approved amendments.

IEEE 802.11 n

IEEE 802.11 n is studying a range of enhancements to both the physical and MAC layers to improve throughput. These include such items as multiple antennas, smart antennas, changes to signal encoding schemes, and changes to MAC access protocols. The current objective of the task group is a data rate of at least 100 Mbps, as measured at the interface between the 802.11 MAC layer and higher layers.

PRACTICAL 6

AIM : To study about GSM architecture and signaling techniques.

- **GSM** stands for **Global System for Mobile Communication.** GSM is an open and digital cellular technology used for mobile communication. It uses 4 different frequency bands of 850 MHz, 900 MHz, 1800 MHz and 1900 MHz . It uses the combination of FDMA and TDMA. This article includes all the concepts of GSM architecture and how it works.

GSM is having 4 different sizes of cells are used in GSM :

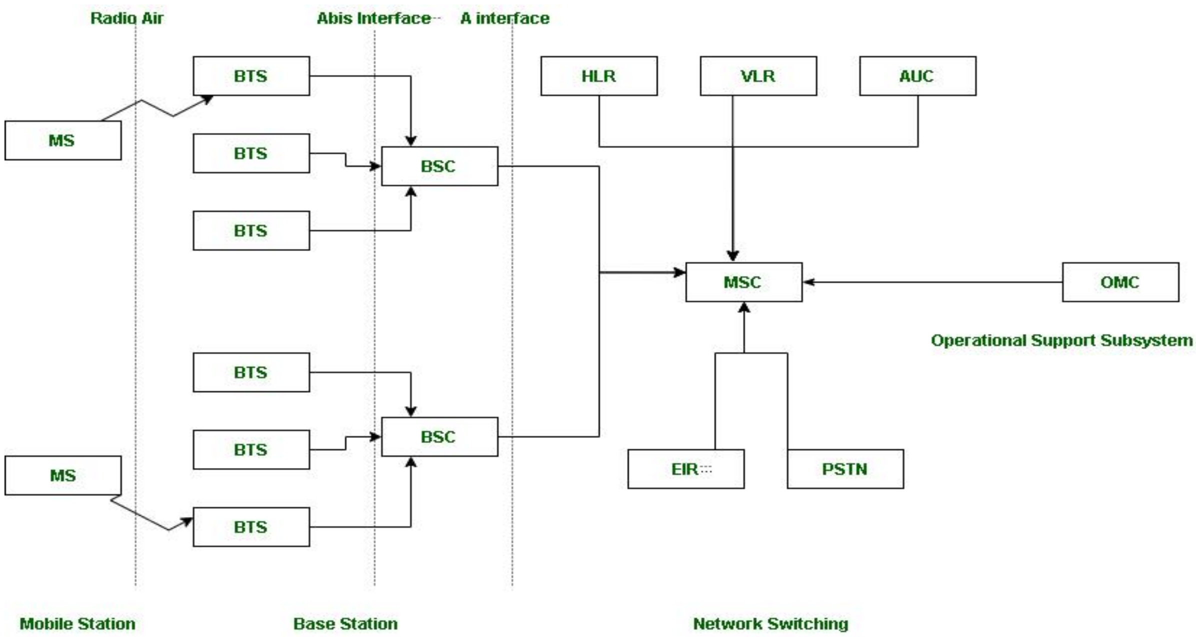
1. Macro : In this size of cell, Base Station antenna is installed.
2. Micro : In this size of cell, antenna height is less than the average roof level.
3. Pico : Small cells' diameter of few meters.
4. Umbrella : It covers the shadowed (Fill the gaps between cells) regions.

Features of GSM are :

1. Supports international roaming
2. Clear voice clarity
3. Ability to support multiple handheld devices.
4. Spectral / frequency efficiency

GSM is nothing but a larger system which is divided into further 3 subsystems.

1. **BSS :** BSS stands for Base Station Subsystem. BSS handles traffic and signaling between a mobile phone and the network switching subsystem. BSS having two components **BTS** and **BSC.**
2. **NSS :** NSS stands for Network and Switching Subsystem. NSS is the core network of GSM. That carried out call and mobility management functions for mobile phone present in network. NSS have different components like **VLR, HLR** and **EIR.**
3. **OSS :** OSS stands for Operating Subsystem. OSS is a functional entity which the network operator monitor and control the system. **OMC** is the part of OSS. Purpose of OSS is to offer the customer cost-effective support for all GSM related maintenance services.



Suppose there are 3 Mobile stations which are connected with the tower and that tower is connected to BTS through TRX, then further connected to BSC and MSC. Let's understand the functionality of different components.

1. MS : MS stands for Mobile System. MS comprises user equipment and software needed for communication with a mobile network. Mobile Station (MS) = Mobile Equipment(ME) + Subscriber Identity Module (SIM). Now, these mobile stations are connected to tower and that tower connected with BTS through TRX. TRX is a transceiver which comprises transmitter and receiver. Transceiver has two performance of sending and receiving.

2. BTS : BTS stands for Base Transceiver Station which facilitates wireless communication between user equipment and a network. Every tower has BTS.

3. BSC : BSC stands for Base Station Controller. BSC has multiple BTS. You can consider the BSC as a local exchange of your area which has multiple towers and multiple towers have BTS.

4. MSC : MSC stands for Mobile Switching Center. MSC is associated with communication switching functions such as call setup, call release and routing. Call tracing, call forwarding all functions are performed at the MSC level. MSC is having further components like VLR, HLR, AUC, EIR and PSTN.

- **VLR :** VLR stands for Visitor Location Register. VLR is a database which contains the exact location of all mobile subscribers currently present in the service area of MSC. If you are going from one state to another state then your entry is marked into the database of VLR.
- **HLR :** HLR stands for Home Location Register. HLR is a database containing pertinent data regarding subscribers authorized to use a GSM network.. If you purchase SIM card from in the HLR. HLR is like a home which contains all data like your ID proof, which plan you are taking, which caller tune you are using etc.
- **AUC :** AUC stands for Authentication Center. AUC authenticates the mobile subscriber that wants to connect in the network.

- **EIR :** EIR stands for Equipment Identity Register. EIR is a database that keeps the record of all allowed or banned in the network. If you are banned in the network then you can't enter the network, and you can't make the calls.
- **PSTN :** PSTN stands for Public Switched Telephone Network. PSTN connects with MSC. PSTN originally a network of fixed line analog telephone systems. Now almost entirely digital in its core network and includes mobile and other networks as well as fixed telephones. The earlier landline phones which places at our home is nothing but PSTN.

5.OMC : OMC stands for Operation Maintenance Center. OMC monitor and maintain the performance of each MS, BSC and MSC within a GSM system.

Three subsystem BSS, NSS and OSS are connected with each other via some interfaces. Total three interfaces are there:

1. **Air Interface :** Air interface is also known as UM interface. Interface between MS and BTS is called as UM interface because it is mobile analog to the U interface of ISDN.
2. **Abis Interface :** It is a BSS internal interface linking with BTS and BSC.
3. **A interface :** It provides communication between BSS and MSC.

Advantages:

Compatibility: GSM is widely used around the world, so it is compatible with many different networks and devices.

Security: GSM offers enhanced security features such as authentication, encryption and confidentiality, which helps to protect the user's privacy and data.

Efficient use of bandwidth: GSM uses a time-division multiplexing (TDM) technique which enables many users to share the same frequency channel at different times, making it an efficient use of the available bandwidth.

Roaming: GSM allows users to roam internationally and use their mobile phones in other countries that use the same GSM standard.

Wide range of features: GSM supports a wide range of features, including call forwarding, call waiting, voicemail, conference calling, and more.

Disadvantages:

Limited coverage: GSM networks may have limited coverage in some remote areas, which can make it difficult for users to make calls or access the internet.

Network congestion: GSM networks may become congested during peak hours, which can lead to dropped calls or poor call quality.

Security vulnerabilities: Although GSM offers enhanced security features, it is still vulnerable to certain types of attacks, such as eavesdropping and spoofing.

Data transfer speed: GSM networks offer relatively slow data transfer speeds compared to newer technologies such as 3G and 4G.

PRACTICAL 7

AIM : To study about Cellular system and related concepts.

- A Cellular Network is formed of some cells. The cell covers a geographical region and has a base station analogous to 802.11 AP which helps mobile users attach to the network and there is an air interface of physical and data link layer protocol between mobile and base station. All these base stations are connected to the Mobile Switching Center which connects cells to a wide-area net, manages call setup, and handles mobility.

There is a certain radio spectrum that is allocated to the base station and to a particular region and that now needs to be shared. There are two techniques for sharing mobile-to-base station radio spectrum:

- **Combined FDMA/TDMA:** It divides the spectrum into frequency channels and divides each channel into time slots.
- **Code Division Multiple Access (CDMA):** It allows the reuse of the same spectrum over all cells. Net capacity improvement. Two frequency bands are used one of which is for the forwarding channel (cell-site to subscriber) and one for the reverse channel (sub to cell-site).

Cell Fundamentals

In practice, cells are of arbitrary shape(close to a circle) because it has the same power on all sides and has same sensitivity on all sides, but putting up two-three circles together may result in interleaving gaps or may intersect each other so order to solve this problem we can use equilateral triangle, square or a regular hexagon in which hexagonal cell is close to a circle used for a system design. Co-channel reuse ratio is given by:

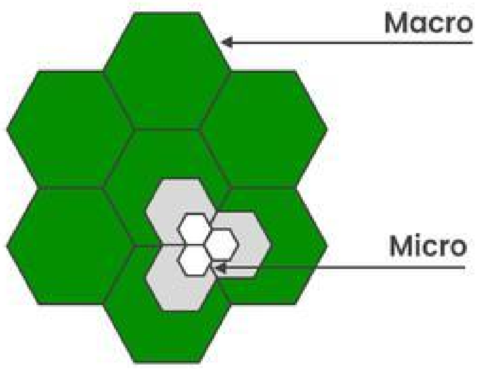
```
DL/RL = Square root of (3N)

Where, DL = Distance between co-channel cellsRL = Cell RadiusN = Cluster Size
```

The number of cells in cluster N determines the amount of co-channel interference and also the number of frequency channels available per cell.

Cell Splitting

When the number of subscribers in a given area increases allocation of more channels covered by that channel is necessary, which is done by cell splitting. A single small cell midway between two co-channel cells is introduced.



Cell Splitting

Need for Cellular Hierarchy

Extending the coverage to the areas that are difficult to cover by a large cell. Increasing the capacity of the network for those areas that have a higher density of users. An increasing number of wireless devices and the communication between them.

Cellular Hierarchy

- **Femtocells:** The smallest unit of the hierarchy, these cells need to cover only a few meters where all devices are in the physical range of the uses.
- **Picocells:** The size of these networks is in the range of a few tens of meters, e.g., WLANs.
- **Microcells:** Cover a range of hundreds of meters e.g. in urban areas to support PCS which is another kind of mobile technology.
- **Macrocells:** Cover areas in the order of several kilometers, e.g., cover metropolitan areas.
- **Mega cells:** Cover nationwide areas with ranges of hundreds of kilometers, e.g., used with satellites.

Fixed Channel Allocation

For a particular channel, the frequency band which is associated is fixed. The total number of channels is given by

Nc = W/B

Where,

W = Bandwidth of the available spectrum,

B = Bandwidth needed by each channels per cell,

Cc = Nc/N where N is the cluster size

Adjacent radio frequency bands are assigned to different cells. In analog, each channel corresponds to one user while in digital each RF channel carries several time slots or codes (TDMA/CDMA). Simple to implement as traffic is uniform.

Global System for Mobile (GSM) Communications

GSM uses 124 frequency channels, each of which uses an 8-slot Time Division Multiplexing (TDM) system. There is a frequency band that is also fixed. Transmitting and receiving do not happen in the same time slot because the GSM radios cannot transmit and receive at the same time and it takes time to switch from one to the other. A data frame is transmitted in 547 microseconds, but a transmitter is only allowed to send one data frame every 4.615 microseconds since it is sharing the channel with seven other stations. The gross rate of each channel is 270, 833 bps divided among eight users, which gives 33.854 kbps gross.

Control Channel (CC)

Apart from user channels, there are some control channels which is used to manage the system.

1. The broadcast control channel (BCC): It is a continuous stream of output from the base station's identity and the channel status. All mobile stations monitor their signal strength to see when they move into a new cell.
2. The dedicated control channel (DCC): It is used for location updating, registration, and call setup. In particular, each base station maintains a database of mobile stations. Information needed to maintain this database is sent to the dedicated control channel.

Common Control Channel

Three logical sub-channels are:

1. Is the paging channel, that the base station uses to announce incoming calls. Each mobile station monitors it continuously to watch for calls it should answer.
2. Is the random access channel that allows the users to request a slot on the dedicated control channel. If two requests collide, they are garbled and have to be retried later.
3. Is the access grant channel which is the announced assigned slot.

Advantages of Cellular Networks

- Mobile and fixed users can connect using it. Voice and data services also provided.
- Has increased capacity & easy to maintain.
- Easy to upgrade the equipment & has consumes less power.
- It is used in place where cables can not be laid out because of its wireless existence.
- To use the features & functions of mainly all private and public networks.
- Can be distributed to the larger coverage of areas.

Disadvantages of Cellular Networks

- It provides a lower data rate than wired networks like fiber optics and DSL. The data rate changes depending on wireless technologies like GSM, CDMA, LTE, etc.
- Macrophage cells are impacted by multipath signal loss.
- To service customers, there is a limited capacity that depends on the channels and different access techniques.
- Due to the wireless nature of the connection, security issues exist.

PRACTICAL 8

AIM: To study about GPRS services.

- **GPRS** is an expansion Global System for Mobile Communication. It is basically a packet-oriented mobile data standard on the 2G and 3G cellular communication network's global system for mobile communication. GPRS was built up by European Telecommunications Standards Institute (ETSI) because of the prior CDPD, and I-mode packet switched cell advances.

GPRS overrides the wired associations, as this framework has streamlined access to the packet information's network like the web. The packet radio standard is utilized by GPRS to transport client information packets in a structured route between GSM versatile stations and external packet information networks. These packets can be straightforwardly directed to the packet changed systems from the GPRS portable stations.

History Of GPRS:
GPRS was one of the main advances that empowered a cell system to interface with Internet Protocol systems, accomplishing across the board reception in the mid-2000s. The capacity to peruse the web from a telephone whenever through "dependably on" data networking, while underestimated in a great part of the world today, was as yet an oddity when it was introduced. Indeed, even now, GPRS keeps on being utilized in parts of the world where it has been too expensive even to consider upgrading cell organize framework to move up to newer alternatives.

According to a study on the history of GPRS development Bernhard Walke and his student, Peter Decker, are the inventors of GPRS – the first system providing universal mobile Internet access.

Goals Of GPRS:

1. Consistent IP services
2. Leverage industry investment in IP
3. Open Architecture
4. Service innovation independent of infrastructure

Services Offered:

1. SMS messaging and broadcasting
2. Push-to-talk over cellular
3. Instant messaging and presence
4. Multimedia messaging service
5. Point-to-Point and Point-to-Multipoint services

Protocols supported:

1. Internet Protocol (IP)
2. Point-To-Point Protocol (PPP)

Benefits Of GPRS:

- **Mobility:**
  The capacity to keep up consistent voice and information interchanges while moving.

- **Cost Efficient:**
  Communication via GPRS is cheaper than through the regular GSM network.
- **Immediacy:**
  Allows customers to obtain connectivity when needed, regardless of location and without a lengthy login session.
- **Localization:**
  Enables customers to acquire data applicable to their present area.
- **Easy Billing:**
  GPRS packet transmission offers an easier to use billing than that offered by circuit switched administrations.

GPRS is an innovation that numerous GPS beacons are using to get up to the minute data with tracking. When the GPS gadget records the information, it would then be able to be transmitted through GPRS to another central location, for example, a PC or through an email. It is the GPRS innovation that takes into consideration ongoing updates to GPS following frameworks. It is this direct GPRS association that gives the client of the GPS system the most reliable information available today.

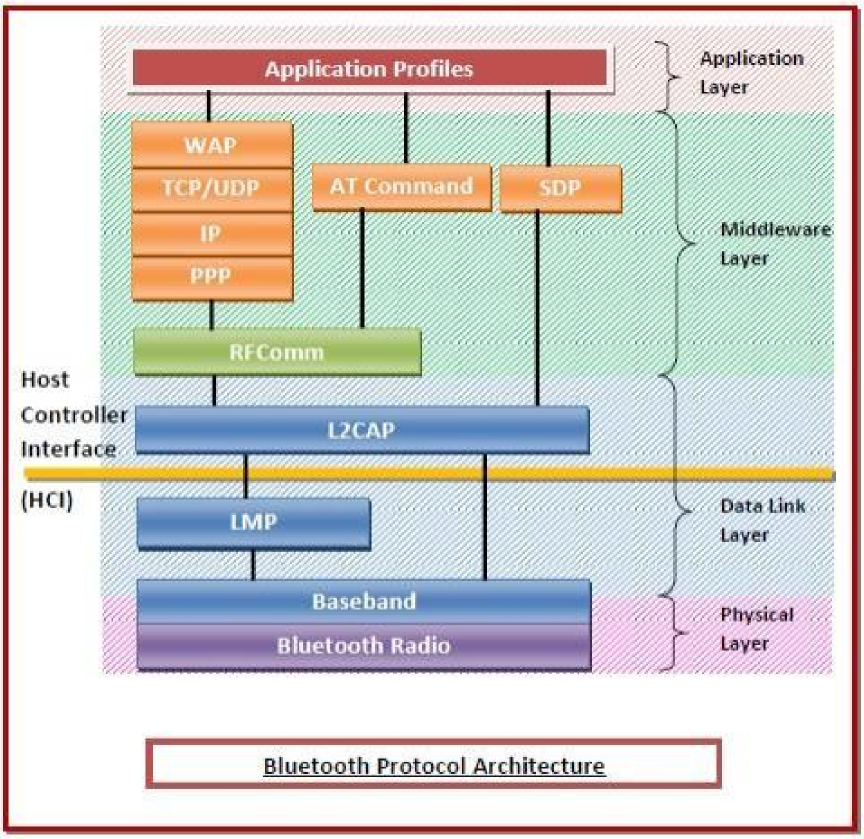
PRACTICAL 9

AIM: To study about Bluetooth architecture.

Bluetooth is an open wireless technology standard for exchanging data over shortn distances (using short wavelength radio transmissions) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS232 data cables. It can connect several devices, overcoming problems of synchronization. Bluetooth is a shortrange wireless network originally intended to replace the cable(s) connecting portable and/or fixed electronic devices. Such a network is also sometimes called a PAN (Personal Area Network) Bluetooth is supposed to got it's name from Harald "Bluetooth" II, King of Denmark 940981.

- The concept was first patented by Ericsson. Currently the Bluetooth trade mark is owned by the Bluetooth SIG, a consortium of companies having stake in Bluetooth
- Key features are robustness, low power, and low cost.

The protocols in the Bluetooth standard can be loosely grouped into the physical layer, data link layer, middleware layer, and application layer as shown in the following diagram −



Bluetooth Protocol Architecture

Protocols in the Bluetooth Protocol Architecture

- **Physical Layer** − This includes Bluetooth radio and Baseband (also in the data link layer.

- **Radio** − This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications, and modulation techniques.
- **Baseband** − This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.

- **Data Link Layer** − This includes Baseband, Link Manager Protocol (LMP), and Logical Link Control and Adaptation Protocol (L2CAP).

- **Link Manager Protocol (LMP)** − LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.
- **Logical Link Control and Adaptation Protocol (L2CAP)** − L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.

- **Middleware Layer** − This includes Radio Frequency Communications (RFComm) protocol, adopted protocols, SDP, and AT commands.

- **RFComm** − It is short for Radio Frontend Component. It provides a serial interface with WAP.
- **Adopted Protocols** − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).
- **Service Discovery Protocol (SDP)**− SDP takes care of service-related queries like device information so as to establish a connection between contending

Bluetooth devices.

- **AT Commands** − ATtention command set.

- **Applications Layer** − This includes the application profiles that allow the user to interact with the Bluetooth applications.

Protocols in the Bluetooth Protocol Stack

- **Core protocols** − This includes Bluetooth radio, Baseband, Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol (L2CAP), and Service Discovery

Protocol (SDP).

- **Cable Replacement Protocol** − This includes Radio Frequency Communications (RFComm) protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP.
- **Adopted Protocols** − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).
- **AT Commands** − ATtention command set

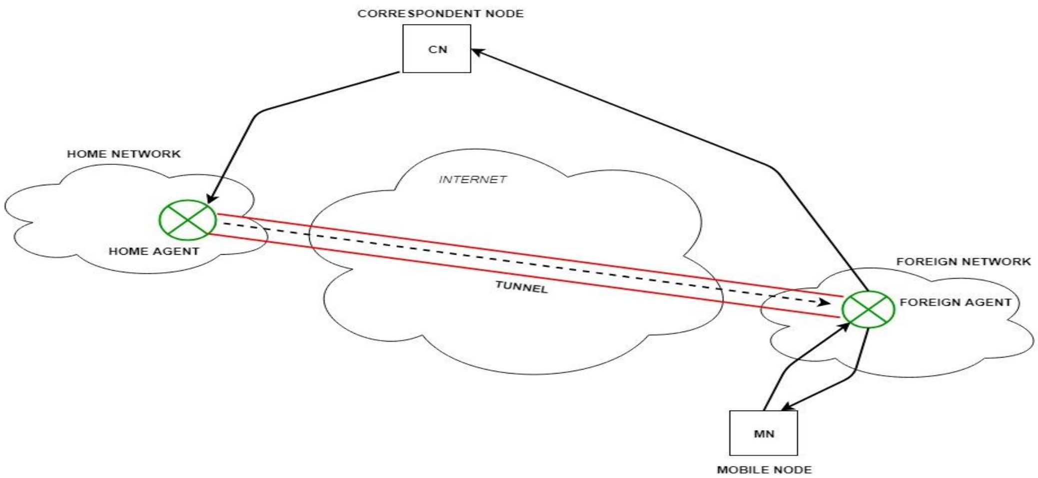
PRACTICAL 10

AIM : To study about Mobile IP.

- **Mobile IP** is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped.

Terminologies:

1. **Mobile Node (MN)** is the hand-held communication device that the user carries e.g. Cell phone.
2. **Home Network** is a network to which the mobile node originally belongs as per its assigned IP address (home address).
3. **Home Agent (HA)** is a router in-home network to which the mobile node was originally connected
4. **Home Address** is the permanent IP address assigned to the mobile node (within its home network).
5. **Foreign Network** is the current network to which the mobile node is visiting (away from its home network).
6. **Foreign Agent (FA)** is a router in a foreign network to which the mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node.
7. **Correspondent Node (CN)** is a device on the internet communicating to the mobile node.
8. **Care-of Address (COA)** is the temporary address used by a mobile node while it is moving away from its home network.
9. **Foreign agent COA,** the COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as a common COA.
10. **Co-located COA,** the COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP.



Mobile IP

Working:

The correspondent node sends the data to the mobile node. Data packets contain the correspondent node's address (Source) and home address (Destination). Packets reach the home agent. But now mobile node is not in the home network, it has moved into the foreign network. The foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling.

Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

Now, the home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address and sends it through the tunnel to the foreign agent. Foreign agent, on another side of the tunnel, receives the data packets, decapsulates them, and sends them to the mobile node. The mobile node in response to the data packets received sends a reply in response to the foreign agent. The foreign agent directly sends the reply to the correspondent node.

Key Mechanisms in Mobile IP:

1. **Agent Discovery:** Agents advertise their presence by periodically broadcasting their agent advertisement messages. The mobile node receiving the agent advertisement messages observes whether the message is from its own home agent and determines whether it is in the home network or foreign network.
2. **Agent Registration:** Mobile node after discovering the foreign agent sends a registration request (RREQ) to the foreign agent. The foreign agent, in turn, sends the registration request to the home agent with the care-of-address. The home agent sends a registration reply (RREP) to the foreign agent. Then it forwards the registration reply to the mobile node and completes the process of registration.
3. **Tunneling:** It establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation. It takes place to forward an IP datagram from the home agent to the care-of-address. Whenever the home agent receives a packet from the correspondent node, it encapsulates the packet with source address as home address and destination as care-of-address.

Route Optimization in Mobile IP:

The route optimization adds a conceptual data structure, the binding cache, to the correspondent node. The binding cache contains bindings for the mobile node's home address and its current care-of-address. Every time the home agent receives an IP datagram that is destined to a mobile node currently away from the home network, it sends a binding update to the correspondent node to update the information in the correspondent node's binding cache. After this, the correspondent node can directly tunnel packets to the mobile node. Mobile IP is provided by the network providers.